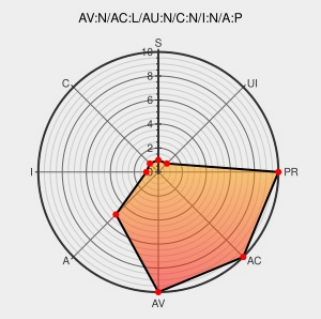
CVE-2005-4720

Published on: 12/31/2005 05:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:20 PM UTC

CVE-2005-4720

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Firefox from Mozilla contain the following vulnerability:

Mozilla Firefox 1.0.7 and earlier on Linux allows remote attackers to cause a denial of service (client crash) via an IFRAME element with a large value of the WIDTH attribute, which triggers a problem related to representation of floating-point numbers, leading to an infinite loop of widget resizes and a corresponding large number of function calls on the stack.

CVE-2005-4720 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 5 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	NONE	PARTIAL

CVE References

Description	Tags	Link
Mozilla Firefox IFRAME Handling Denial Of Service Vulnerability	Exploit, cve.report (archive), text/html	BID 15015
LinkedIn	Exploit, Vendor Advisory, www.security-protocols.com, text/plain, Inactive Link, Not Archived	MISC www.security-protocols.com/advisory/sp-x19-advisory.txt
Secunia - Advisories - Mozilla Firefox Iframe Size Denial of Service Weakness	Patch, Vendor Advisory, web.archive.org	SECUNIA 17071

303433 – CVE-2005-4720 Firefox 1.0.6 segfaults on this malformed .html page	bugzilla.mozilla.org text/html	CONFIRM bugzilla.mozilla.org/show_bug.cgi?id=303433
SecurityTracker.com Archives - Mozilla Firefox Buffer Overflow in Processing IFRAME Widths May Let Remote Users Execute Arbitrary Code	Exploit securitytracker.com text/html	SECTRACK 1015011
No Description Provided	Exploit Vendor Advisory web.archive.org text/html Inactive Link Not Archived	MISC security-protocols.com/modules.php?name=News&file=article&sid=2978

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Mozilla	Firefox	1.0.6	All	All	All
Application	Mozilla	Firefox	1.0.7	All	All	All
Application	Mozilla	Firefox	1.0.6	All	All	All
Application	Mozilla	Firefox	1.0.7	All	All	All

cpe:2.3:a:mozilla:firefox:1.0.6:*:*:*:*:*:*:*

cpe:2.3:a:mozilla:firefox:1.0.7:*:*:*:*:*:*:*

cpe:2.3:a:mozilla:firefox:1.0.6:*:*:*:*:*:*:*

cpe:2.3:a:mozilla:firefox:1.0.7:*:*:*:*:*:*:*

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→